First Data

A First Data White Paper

Selecting a Secure and Compliant Prepaid Reloadable Card Program

Merchants and other distributors of prepaid general purpose reloadable (GPR) cards should review program compliance as an integral part of the overall value proposition of a prepaid product offering since not all programs are created equal.

By Tom McGimpsey
Vice President, Operations

Introduction

In today's competitive business environment, merchants and other consumer-facing organizations are looking for ways to provide a value-added prepaid card that results in increased retail use and enhanced customer loyalty. Branded prepaid general purpose reloadable (GPR) cards provide underbanked and unbanked consumers with the convenience, flexibility, safety and prestige of a network-branded card (e.g., Visa™, MasterCard™, Discover™ Network and others) for making everyday purchases, obtaining cash at ATMs and paying bills. Unlike conventional prepaid cards, prepaid GPR cards allow customers to reload them with additional funds—and even set up direct deposits to them. Prepaid GPR cards address a variety of consumers' needs, and they utilize the infrastructure of existing payment networks similar to credit and debit cards. Changes in the economic climate and in consumer spending habits have invigorated the usage of prepaid GPR cards, and according to a 2008 Mercator report, GPR load amounts will grow by over 50 percent annually through 2011. The rising popularity of GPR cards is making them an increasingly attractive component of retail prepaid product portfolios.

Loading and Reloading a GPR Card

Prepaid GPR cards can be purchased by consumers at a retail location or online. A purchase fee is paid and an initial load amount is placed on the card. The card is later activated as a reloadable card when the cardholder calls the customer service number (or logs on to the secure Web site) to provide personal information as required by the USA Patriot Act. Some programs will then send the customer a new card with the customer's name fully embossed on the card.

Merchants and other prospective distributors of prepaid GPR cards need to holistically examine each component of a planned GPR program to ensure it will launch and grow successfully. In addition to design, scalability and reliability concerns, questions regarding the program's compliance should also be asked. Have the various components of the program (e.g., card design and issuance, card loading, transaction processing, cardholder communications and marketing, periodic statements, notice requirements, receipts, disputes, chargebacks) been designed to meet or exceed federal, state and industry requirements? This white paper is intended to facilitate discussions with current or prospective prepaid program managers (the non-bank entities that set up and operate prepaid programs) on fundamental compliance questions related to:

- → Data Protection
- → Regulatory and Industry Compliance
- → Integrated Risk and Fraud Management
- → Program Design Parameters

A competent, experienced prepaid program manager will be able to concisely address such questions and can outline the compliance roles and responsibilities of the key participants in the prepaid value chain (i.e., the financial institution card issuer, the program manager, the processor and the merchant/seller). A keen understanding of compliance requirements in the prepaid market will also allow the parties to quickly address changes to the program to meet market demands and opportunities in a timely manner.

Data Protection

Protecting a cardholder's account information and personal data is critical to providing a quality prepaid GPR product. Prepaid GPR cards require a greater level of data protection than conventional prepaid offerings, in part, because of the personal information that becomes associated with them when a customer activates it as a reloadable card. Prepaid GPR cards are also usually used for a longer period of time than traditional prepaid instruments, and are likely to carry higher balances—both of which can make them more probable fraud targets. Stories of data compromises and electronic fraud permeate the daily news and are the focus of consumer concerns, and accordingly, regulators' attention. As such, merchants will want to ask their prepaid program manager some key data protection questions:

- → Are the systems and processes that handle cardholder data PCI[1] compliant?
- → Does the processor have an information security policy[2] that outlines comprehensive data security protections?
- → Do the parties have a robust privacy policy that is Gramm-Leach-Bliley Act[3] (GLB) compliant, and one that protects cardholders' personally identifiable information (i.e., name, address, Social Security number and date of birth)?

[1] PCI refers to the Payment Card Industry Data Security Standards. Notably, some states have incorporated (or plan to incorporate) some of these requirements in state legislation, such as encryption. Payment networks also require PCI assessments and compliance.

[2] Many information security policies will address areas such as organizational security, asset classification and control, personnel security, physical and environmental security, communications and operations management, access controls, system development and maintenance, business continuity management, compliance and detailed requirements for external access, Web sites, virus scanning, encryption, intrusion detection, etc

[3] The Gramm-Leach-Bliley act requires financial institutions to provide clients with a privacy notice that explains the information the company gathers about clients, where this information is shared, and how the company safeguards that information.

- → Do the parties have a data incident response plan to quickly address, mitigate and report potential data incidents should they occur?
- → Do the parties have a dedicated corporate-wide information security team and privacy officer?

While this list is not comprehensive, it provides the basis for a beginning dialogue with your prepaid program manager. Succinct answers to these questions will offer the merchant assurance that the prepaid program manager takes data protection seriously and has built these safeguards into the product offering. Industry best practices also play a key role in mitigating even the possibility of a data breach. These practices include hashing or truncating the viewable card number even beyond PCI requirements, having account numbers that are different from card numbers, having additional forms of cardholder authentication and other measures. Protecting your customers' data should be at the heart of any prepaid GPR program.

Regulatory and Industry Compliance

Prepaid GPR cards and payroll cards[4] are considered by many to be the most regulated products in the prepaid card industry. Prepaid GPR cards are issued by regulated financial institutions that are subject to stringent federal review, examination and oversight. In addition, a merchant selling such cards might need to be registered as a licensed money transmitter (or be an agent of a licensed money transmitter) in certain states. Payment networks such as Visa, MasterCard, Discover and others impose additional policies, operating rules and best practices that apply to all participants in the prepaid value chain. The regulatory and industry requirements are significant, and you will want an experienced prepaid program manager to handle the details. Listed below are just some of the areas that should be reviewed and discussed:

- → An Anti-Money Laundering (AML) program adopted under the Bank Secrecy Act and the USA Patriot Act to prevent, detect and report potential money laundering. Such a program should have the following four key components:
    1. The designation of a compliance officer
    2. Written internal controls and procedures for many of the items listed below
    3. An AML training course for employees who have day-to-day responsibility for the sale, loading and redemption of prepaid GPR cards
    4. An independent annual review of the AML program
- → A Customer Identification Program (CIP) that collects and verifies cardholder information as part of the card enrollment process and uses either a third-party database check or requires physical examination of government-issued documents
- → Consumer notification requirements throughout the product's life cycle (e.g., USA Patriot Act notices, money transmitter notices, GLB notices, privacy notices, etc.)
- → An Office of Foreign Assets Control (OFAC) screening process in which cardholder information is checked against the federal list of oppressive governments, international terrorists, narcotics traffickers and other specifically designated persons
- → Suspicious-activity monitoring (post-transaction) of the prepaid account once the card is activated, and the reporting of unusual activity to FINCEN[5]
- → Currency transaction reporting to the federal government, and the collection of certain information from the cardholder for the sale of monetary instruments

[4] For a discussion of payroll card compliance, please see First Data's white paper titled "Achieving Electronic Pay for All Employees" dated July 30, 2008, by Mark Smith and Todd Lasher.

[5] The Financial Crimes Enforcement Network (FINCEN) is a bureau within the Department of Treasury.

- → Reporting of transactions to states where adherence to state money transmission statutes might be required or advisable
- → Notification and escheatment laws related to abandoned property in prepaid accounts
- → Dispute and chargeback procedures and extension of Regulation E[6] protections to cardholders for unauthorized transactions
- → Complying with applicable National Automated Clearing House Association (NACHA) requirements as they relate to ACH transmission of funds to and from the prepaid GPR card
- → Consumer disclosures that comply with federal and state requirements (including bank authority guidelines and FTC laws regarding unfair or deceptive practices)
  - For example, some GPR card programs allow consumers to "Withdraw from Checking" or "Withdraw from Savings" at an ATM. Allowing for the "Withdraw from Savings" option may inadvertently and incorrectly imply that the prepaid account is an interest-bearing savings account
- → Adherence to the various payment network policies, operating rules and best practices

While all market participants will claim that their prepaid GPR programs are fully compliant, the level and extent of that compliance will be demonstrated by the degree to which it is engrained and incorporated into every facet of the program. An experienced prepaid program manager can map the various requirements against each phase of the card's life cycle (from issuance to final use).

Integrated Risk and Fraud Management

Since fraud patterns related to unauthorized transactions are always changing and new fraudulent schemes can quickly emerge, merchants will want to understand how the prepaid GPR card program has integrated risk and fraud management to provide a balanced approach to cardholder protection. Accordingly, the overall framework of risk and fraud management tools and strategies should include:

- → A risk review of the specific program parameters for the card (see discussion below)
- → Utilization of the information from the AML suspicious-activity monitoring (discussed above) since such activity could indicate general fraud activity
- → Real-time fraud detection and response tools if the product is expected to be used for an extended period of time, which is the case with prepaid GPR cards

With respect to this last point, progressive prepaid program managers are looking at ways to offer real-time fraud information and monitoring similar to what is offered today for credit and debit cards. These services often employ Fair Isaac Corporation's Falcon™ Fraud Manager neural network-based modeling technology, which provides a cardholder profile and transaction-based scoring. The benefit of real-time fraud monitoring is to:

- → Detect fraud faster and more efficiently
- → Deal efficiently and effectively with large volumes of complex data
- → Adapt to fit new and emerging fraud patterns
- → Quickly stop fraud and loss exposure with a consistent review of all transaction activity

[6] Regulation E protections generally do not apply to Prepaid GPR cards; however, they do apply to payroll cards since the law was expanded on July 1, 2007.

Notably, the Falcon Fraud Manager solution (which is used by First Data's Fraud Risk Identification Service) incorporates data from millions of transactions across hundreds of issuers to leverage powerful knowledge about fraud patterns (specific to a region and portfolio) for improved fraud detection, no matter the size of your portfolio.

While not all financial institutions offer such services for prepaid GPR cards, it is worth asking what capabilities exist. Whatever services are available, it is critical that fraud is centrally managed by either the financial institution, the prepaid program manager or the processor.

Prepaid GPR Program Design Parameters

Lastly, merchants will want to work with a prepaid program manager who has an in-depth knowledge of the various program design parameters that comprise a successful prepaid GPR card product offering. The program parameters, if designed correctly, can mitigate the chances that the card will be used for money laundering and could reduce the amount of fraud that can occur. Since some of these parameters are reflected in the cardholder "Terms and Conditions," it is important to get them right the first time and to review them periodically. Best practices include:

- Restricting the loads (both daily and monthly) to amounts and frequencies that are reasonable and appropriate based on the type of card and cardholder needs. In particular, cash funding and ATM cash withdrawals should have daily limits in order to address potential money laundering concerns. Notably, credit card loads and ACH loads are less problematic
- Implementing daily spend (or velocity) limits that are appropriate and prevent the rapid drain of funds should fraud occur
- Establishing a maximum balance for the card
- Imposing multiple-card restrictions for the same name, address (postal, e-mail or IP address) or Social Security number
- Restricting the number of allowable replacement cards
- Limiting offline/stand-in-processing (STIP) transactions

Conclusion

Prepaid general purpose reloadable cards are a rapidly growing payment instrument that offers compelling benefits to consumers, and significant incremental revenue opportunities to merchants and other organizations. They also require unique security and compliance considerations—but by understanding the details surrounding data protection, regulatory and industry compliance, integrated risk and fraud management, and program design parameters, you will be well positioned to select the appropriate partners to help you implement a prepaid GPR card program that is effective, compliant and protective of the consumer.

Data Protection
Regulatory & Industry Compliance
Integrated Risk & Fraud Management
Program Design Parameters

First Data

The Global Leader in Electronic Commerce

First Data is a recognized leader in the prepaid card industry, and has a dedicated team of industry and compliance professionals that deliver secure, successful market-leading prepaid solutions to customers of all sizes. For more information on First Data's prepaid offerings, please visit: firstdata.com/product_solutions/prepaid_solutions.

About The Author

Tom McGimpsey, vice president of Operations at First Data, is responsible for regulatory and industry compliance operations for stored-value gift, prepaid gift, prepaid reloadable and payroll card programs. Mr. McGimpsey is also the privacy officer for First Data Prepaid and provides guidance on new product development. He was formerly an executive for a publicly traded IT equipment and software company and was in charge of legal/compliance and international business development. Mr. McGimpsey has a master's degree in business administration and is a registered attorney.

For more information, contact your
First Data Sales Representative
or visit firstdata.com.